白山云云聚合产品解决方案

总叙：

白山云科技有限公司为国内首家互联网云链服务提供商，以数据内容为服 务核心，为企业客户提供高效数据内容应用与交换的定制化服务。自2015年4月成立以来，白山以云分发为切入点，在云后服务市场上迅速崛起，云聚合是白山云的全新产品，围绕动态接口为企业提供一系列服务，包括数据接口构建、接口适配、接口加速、接口安全保护和接口大数据分析。云聚合可以帮助打造OpenAPI平台，有效提高接口API的访问速度，同时在大并发的情况下保障接口的正常访问，适用于电商、金融、传统企业、互联网企业等大业务量的场景。

功能：

云聚合包含以下核心功能：

API构建	API自动构建	通过数据自动生成API
API适配	接口定义	通过swagger定义标准API
	接口转换	将不同接口适配统一
API加速/后端保护	L2 Cache	动态接口cache加速
	异步化（全异步化/半异步化）	接口异步化保护
	WebSocket协议转换	实时信息接口加速
API安全	API HTTPS转化	HTTP=>HTTPS转换
	API认证/流控	接口身份认证，流量控制
	API HTTP防火墙（CC防火墙）	CC防火墙，防护多种接口攻击
API分析	大数据分析	统计分析

其中API HTTP防火墙（CC防火墙）功能如下：

识别	自定义日志推送
	实时分析
	自定义识别规则
拦截	分域名拦截
	内核拦截
	灰IP自动跳转验证码
	自定义拦截行为

API HTTP防火墙（CC防火墙）能够防护的攻击类型如下：

负载消耗攻击	HTTP flood

CPU消耗攻击	随机构造攻击
	404穿透攻击
连接数消耗攻击	HTTP发包慢速攻击
	HTTP收包慢速攻击
流量消耗攻击	异常header包攻击
	异常body包攻击
其他	高频验证码校验
	经验抓站UA

API HTTP防火墙（CC防火墙）性能指标如下：

部署环境	10台* 24核 128G内存 Centos 6.5
每分钟处理请求数	6000万

特点：

白山云聚合产品是围绕动态接口打造的包括构建、加速、防护、安全、分析在内的一系列产品，它对比友商的产品，具有以下独有特点：

架构特点：	公有云/私有云部署	白山云云聚合同时支持公有云、私有云两种部署模式，企业既可以使用白山云聚合公有云服务，对于某些安全性要求高的企业，又可以快速的将云聚合产品部署在企业内部
	软件实现	白山云聚合可以部署在任意Linux架构的服务器上，不依赖特殊硬件，基于通用开源软件，方便部署/维护，不存在绑定关系
	API接口旁路防护	对于API防护，白山的HTTP接口防火墙具有独有的旁路防护模式，可以以旁路模式工作，不影响业务主体流程，也不影响业务主体可用性
功能特点：	API L2 Cache	支持接口毫秒级cache，可以在不影响用户体验的情况下，提高接口响应速度
	API异步化	在大并发情况下，自动将请求异步队列化，并自动控制并发度，保护后端服务正常
	WebSocket协议转换	可以将HTTP接口转换为WebSocket事件驱动接口，在降低后端负载的前提下，大大提高接口的实时响应，提升用户体验
技术特点：	无状态对等部署	云聚合采用无状态对等部署，没有单点，保证服务高可靠性

	防火墙内核拦截技术	不同于传统的7层防火墙，白山云HTTP防火墙具有3层拦截技术，工作在Linux Kernel网络栈，性能比7层防火墙高一个数量级
	流式大数据分析	基于Storm流式实时大数据分析，可以几秒内即做出分析响应
	防火墙防误拦技术	针对公司上网时，同一个出口IP产生大量的正常访问行为这种情况，白山云拥有一套基于用户特征分布模式的算法分析，可以区别出攻击行为还是正常行为，最终提供准确拦截
	包丢弃技术	传统的7层防火墙的返回HTTP错误码或者RST拦截从本质上来讲并没有增加攻击者的攻击成本，而白山云HTTP防火墙使用独有的包丢弃技术，拦截攻击IP后，攻击者会发生超时现象，大大增加攻击者的攻击成本

对比友商的核心优势：

- 私有云部署，支持私有云模式部署在企业内部
- 旁路防护，不影响主干业务，极端情况：假设云聚合服务器全部宕机，也不原有业务工作
- 大数据分析，实时分析算法，对于HTTP拦截，攻击发生后几秒内拦截
- 结合业务实现零误拦，深度结合业务特点（如cookie、uid），做到零误拦率
- 包丢弃技术，从而实现防范的同时大大增加攻击者成本
- 后端异步化保护，通过L2 cache、异步化等模式，保护秒杀高并发活动下的后端正常运行

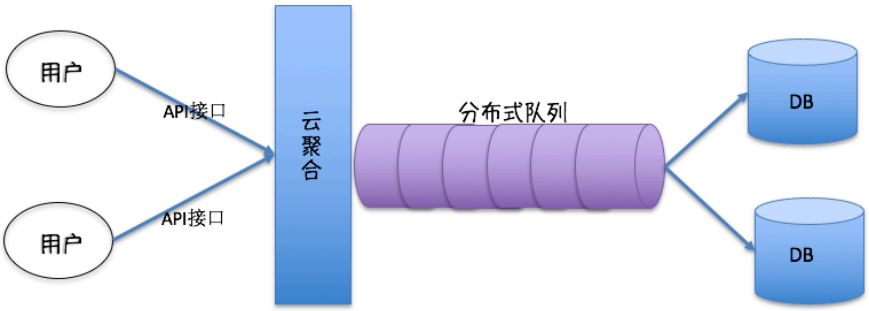
典型应用场景：

1，促销活动导致大并发，接口响应慢？

促销活动时，有时候大量用户请求同一个（或者少数几个）产品信息，大量的高并发查询导致接口变慢。
利用L2 Cache，为接口增加毫秒级cache，这样可以将数据cache的从业务cache层，前移到负载均衡层，从而避免数据高热点引起的响应慢。另外，为接口增加cache，通过设定合理的cache规则，可以有效提高接口的cache命中率，进而提高接口的响应速度。

2，秒杀活动导致后端服务（如数据库）不稳定？

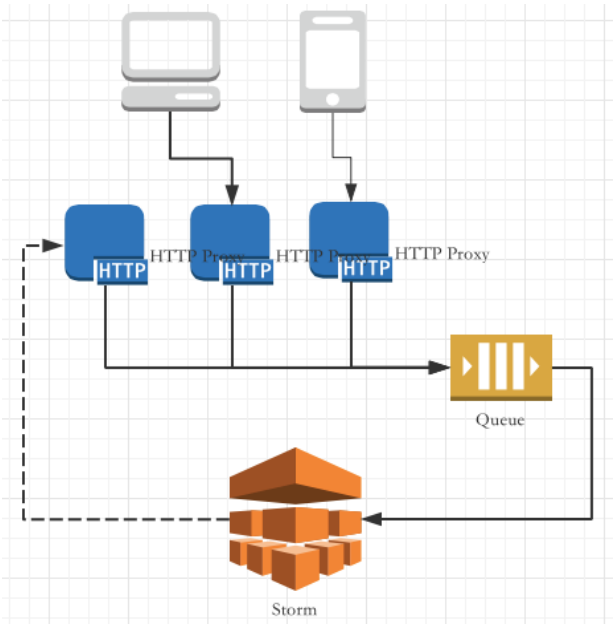
进行秒杀活动时，大量的并发有时候会导致后端压力过大，尤其对于常见的瓶颈服务（如数据库），一旦数据库压力过大，必然导致接口变慢，进而出现页面卡顿的现象，最终影响用户体验。
利用API接口异步化保护，可以保证秒杀活动再大的并发，后端服务仍然正常运行。



如图所示，当用户并发访问增加时，白山云聚合服务会自动将用户请求放入队列，而不是直接转给后端DB服务。队列的并发度和后端DB服务能够承载的并发度匹配，这样再大的并发，也可以完美保证后端DB接收到的并发度可控。

3，恶意用户进行HTTP攻击，进行恶意刷单？

针对恶意用户的HTTP攻击（如刷单），白山云聚合HTTP防火墙（CC防火墙）能够收集用户的访问日志，通过Storm流式大数据分析，分析出攻击IP，并且以旁路的方式在Linux Kernel层进行拦截，保证业务的正常开展。

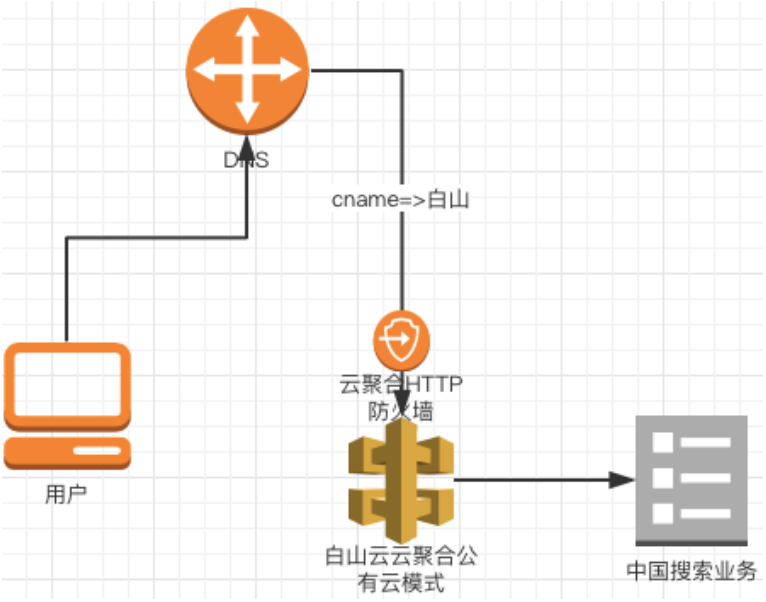


如图所示，业务方将请求日志推送到队列，Storm分析集群可以在几秒内根据特征算法分析出攻击IP，并且反馈到部署在被保护服务器上的拦截器，拦截器以旁路模式运行（不影响主体业务），并最终将攻击IP在3层进行拦截。

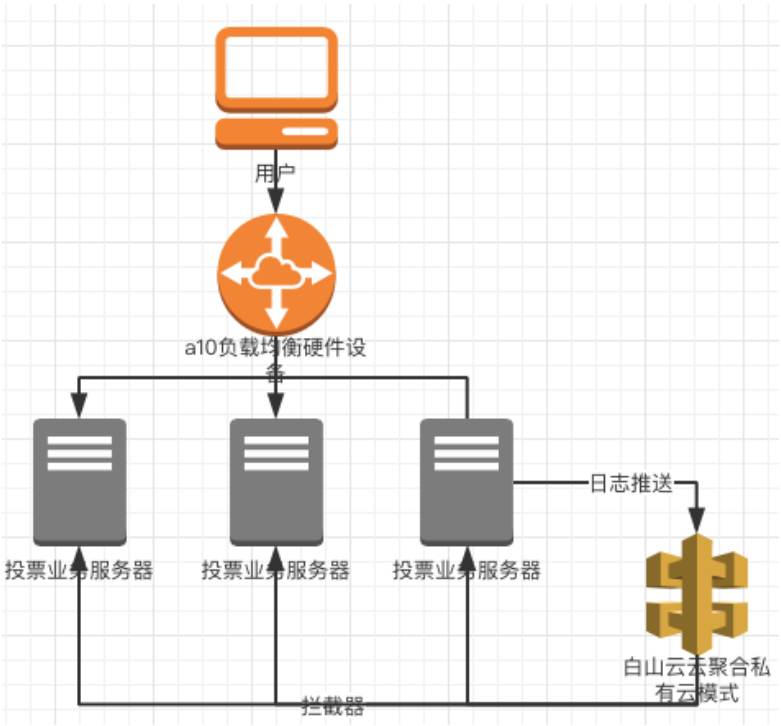
测试案例：

1，中国搜索（国搜）应用云聚合HTTP防火墙防范搜索词穿透攻击

中国搜索是一家提供搜索的大型互联网公司，经常面对搜索词穿透攻击，即攻击者构建偏僻的搜索词进行搜索，因为搜索接口属于动态API接口，一般CDN无法保护，这样的搜索请求会穿透到后端，而又因为搜索词很生僻，导致cache无法命中，进而白白消耗服务器资源。
为了解决这个问题，中国搜索应用了白山云云聚合的HTTP防火墙，国搜采用的是公有云模式，即将把被攻击的域名cname给白山，白山通过流式大数据算法分析，可以实时得出攻击IP，并最终将这些IP进行拦截，保护了业务的正常运行。



2，中国日报应用云聚合HTTP防火墙应对恶意投票行为



中国日报（ChinaDaily）是一家知名的国内媒体，并且在国外也有一定影响力，中国日报经常承办地方各个机构的投票业务，这些投票业务刷票行为十分严重，刷票容易导致：1，服务器负载增高导致服务不正常；2，影响投票结果的公平性，导致业务方不满意。

针对这个情况，中国日报部署了白山云云聚合的HTTP防火墙，他们采用的是私有云模式，即旁路拦截模式。HTTP防火墙位于中国日报最前端a10负载均衡后面，通过分析传递来的HTTP日志，利用算法区分正常投票和恶意刷票，保护web服务器正常运行。
部署了白山云云聚合HTTP防火墙，有效的防止了刷票现象的发生，为客户带来了好评。

3，掌上贵金属公司应用云聚合API异步队列化保护后端数据库服务

掌上贵金属是上海一家专注于纸黄金交易的互联网创业公司，提供移动端的App贵金属交易，他们面临一个问题，到交易密集时期，因为大量用户发起查询行情请求，经常导致数据库压力过大从而出现卡顿的现象。
掌上贵金属采用了白山云云聚合的私有云部署模式，应用了API接口异步化的功能，针对实际的后端接口并发承载力设定了队列并发度，并开启了智能异步化模式。当并发增加时，异步化自动选择起作用，这时，用户的请求不再直接转给后端数据库，而是推送到分布式队列中异步的处理，队列的并发程度和后端数据库的实际处理能力匹配，这样再大的请求量也可以保证后端服务正常。